JOHN S. LEONARDO
United States Attorney
District of Arizona

FREDERICK A. BATTISTA
Assistant U.S. Attorney
Maryland State Bar Member
Two Renaissance Square
40 N. Central Ave., Suite 1200
Phoenix, Arizona 85004
Telephone: 602-514-7500
Email: fred.battista@usdoj.gov
Attorney for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

United States of America, Plaintiff, vs. Daniel David Rigmaiden, Defendant.	CR-08-814-001-PHX-DGC STIPULATION RE FORENSIC COPIES OF DIGITAL EVIDENCE

The United States of America, by and through undersigned counsel, and defendant, DANIEL DAVID RIGMAIDEN, Pro Se, hereby stipulate and agree as follows:

1. On August 3 and 4, 2008, federal law enforcement officers seized the following digital devices (collectively, the "Original Digital Devices") from 431 El Camino Real, Apartment 1122, Santa Clara, California 95050, and Storage Unit No. A-47, CDB Indoor Mini Self-Storage, 570 Cinnabar Street, San Jose, California 95110, while executing federal search warrants in the course of the investigation of this case:

a. IBM ThinkPad laptop (SN LV-C4398) containing Hitachi 100GB hard disk drive (S/N MPCZN7Y0J7N51L),

b. External hard drive enclosure containing Seagate 500GB hard drive (SN 3PM07D08),

c. External hard drive enclosure containing Toshiba 100GB hard drive

(SN 36901970S),

d. Acer MS2180 laptop (SN LXAA6050876090F641KS00) containing Samsung 40GB hard disk drive (S/N S03WJ30L218364),

e. External hard drive enclosure containing Toshiba 100GB hard drive (SN 36901974S).

f. Dane-Elec Blue 1GB Thumbdrive,

g. SanDisk 2GB Compact Flash Ultra II Memory Card,

h. Seagate 250GB Hard Drive (S/N 5QE1W2CP),

i. SanDisk TransFlash 64MB Memory Card,

j. Sony CyberShot Camera (S/N 506621), and

k. Sony Memory Stick Pro Duo Memory Card.

Note for items f-k, no evidence was collected by the United States and all forensic images have been deleted.

2. Thereafter, the government made complete duplicates of the Original Digital Devices listed in ¶ Nos. 1(a) - 1(e) above. The files contained within the duplicates are exact and accurate copies of the files contained on the Original Digital Devices at the time they came into the government's possession. Other than for the Master File Tables contained on the Original Digital Device named "filesalot.dcv," the file system metadata (*e.g.*, "file last access dates") were exact and accurate copies of the file system metadata contained on the Original Digital Devices prior to the materials coming into the government's possession. However, for the Original Digital Device named "filesalot.dcv," the "file last access date" file system metadata corresponding to an unconfirmed number of files were changed on August 3-4, 2008, as a result of the government using WinRAR and MD5Summer to access and copy the noted files via direct access to the Original Digital Device file system. Consequently, the government's duplicates of the "filesalot.dcv" contain an unconfirmed number of files with "file last access date" file system metadata reflecting the dates/times the government accessed the files on the Original Digital Device after defendant was arrested and in custody. While the

duplicates of "filesalot.dcv" have an unconfirmed number of files with "file last access date" file system metadata reflecting the dates/times the government accessed the file system on the Original Digital Device, all of the files from "filesalot.dcv" that the government is keeping as Necessary Digital Evidence are confirmed to have "file last access date" file system metadata reflecting the dates/times the government accessed the files on the Original Digital Device after defendant was arrested and in custody.

3. After the creation of the duplicates, the government identified digital data the government believed was necessary to prosecute defendant. The government isolated and copied the necessary data from its duplicates (collectively, the "Necessary Digital Evidence"). Copies of the Necessary Digital Evidence have been provided to defendant in discovery in this case. After providing the Necessary Digital Evidence in discovery, the government saved (1) the Necessary Digital Evidence, and (2) all computer forensic reports and associated files of which the government wishes to keep,[1] into a DriveCrypt encrypted container file named "Digital_Evidence.dcv" having the following SHA-256 hash digest value:[2]

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016

(hereafter the "Necessary Digital Evidence Container File"). To prevent questions or later

---

[1] The noted forensic reports and associated files resulted from the government's use of EnCase and/or other computer forensic software while examining the duplicates of the Original Digital Devices.

[2] SHA-256, as well as SHA-1, SHA-224, SHA-384, SHA512, SHA-512/224 and SHA-512/256, are all "iterative, one-way hash functions that can process a message to produce a condensed representation called a message digest. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest." National Institute of Standards and Technology, FIPS PUB 180-4, *Federal Information Processing Standards Publication: Secure Hash Standard (SHS)* (Mar. 2012), p. 3. In this case, the "message" is the totality of the Necessary Digital Evidence Container File. The resulting "message digest" will change if files are added to or removed from the Necessary Digital Evidence Container File—thus, making changes detectable.

disputes regarding what constitutes Necessary Digital Evidence, the government provided defendant with an exact copy of the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016.

This stipulation does not establish that the Necessary Digital Evidence is data falling within the scope of any warrant executed by the government in this case.

4. Defendant has requested that the government destroy the data on the Original Digital Devices and on the duplicates using the process described in ¶ No. 5 below. The originals and duplicates include (1) all data on all copied Original Digital Devices, (2) all forensic images of Original Digital Devices, (3) WinRAR archive(s) made during live acquisitions of data contained on Original Digital Devices, (4) the three virtual machine clones of the entire computer system (which are themselves complete copies of all Original Digital Devices) which are now all in the possession of IRS-CI (one having been returned to IRS-CI by the FBI), (5) originals and duplicates of all DriveCrypt encrypted container files including:

i. filesalot.dcv;

ii. filesalot_bak_3-31-2008.dcv;

iii. filesalot_bak_3-1-2008.dcv;

iv. filesdone60_1.dcv;

v. filesdone60_2.dcv; and

vi. T_drive.rar

which originated from the Original Digital Devices, (6) all MD5 or other hash digests (*i.e.*, the digital fingerprints recorded on August 3-4, 2008 and possibly on other dates) taken of files on Original Digital Devices and duplicates, (7) all evidence cache files, automatic backup files, case files, reports, case databases, backup files, temporary file folders, and Analysis Reports resulting from government use of EnCase, AccessData FTK, and/or other computer forensic software—as well as all other residual data resulting from any forensic analysis—other than what is saved into the Necessary Digital Evidence

Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016,

and (8) all other copies of data originating or created from Original Digital Devices which are not copies of data contained within the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016.

5. While destroying data on the Original Digital Devices and on the duplicates, defendant requests that the government use a secure drive wipe process consisting of (1) writing each bit of data on each relevant hard drive three (3) times with random bits of data, *i.e.*, data not merely consisting of zeros, (2) overwriting the file and folder properties (name, dates, size, *etc.* saved within the file system metadata) corresponding to deleted files, and (3) reformatting the drives so as to erase the Master File Tables (MFTs), File Allocation Tables ("FATs"), or equivalent metadata repositories corresponding to the applicable file system. After the destruction/returning process, if additional seized data not consisting of data contained within the Necessary Digital Evidence Container File is located on any storage device in the government's possession by a case agent, prosecutor, or other government actor involved in CR08-814-PHX-DGC, defendant requests that the data be deleted or destroyed without documenting the data in government records or sharing the data to be destroyed with any other agent, agency, or entity within the government, with any other jurisdiction, or with any private party, and that defendant be notified of its deletion or destruction of the located data.

6. Once the data contained on the Original Digital Devices and on the duplicates are destroyed, defendant requests that the government personnel who conducted the destruction process issue a signed report to defendant detailing the destruction process that occurred. The report will include (1) a list of all Original Digital Devices and duplicates that were subject to the data deletion process described in ¶ No. 5 above, (2) an accounting of how the data contained on Original Digital Devices and duplicates was destroyed, (3) an indication that all data contained on the eight (8) categories of Original

Digital Devices and on the duplicates listed in ¶ No. 4 above were destroyed, (4) an indication that, to the best of the government's knowledge, the only copied data currently in its possession consists of the Necessary Digital Evidence saved within the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016,

and (5) an indication that no data within the destroyed data, i.e., data not contained in the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016,

was previously physically shared with any other agent, agency, or entity within the government, with any other jurisdiction, or with any private party.

7. Acting in accordance with defendant's requests contained in ¶ Nos. 4-6 above, the government will (1) destroy the data contained on the Original Digital Devices and on the duplicates, (2) create the requested report, and (3) make the requested notifications. In exchange for acting in accordance with defendant's requests contained in ¶ Nos. 4-6 above, and upon the condition that no destroyed data was previously physically shared with any other agent, agency, or entity within the government or with any other jurisdiction, defendant stipulates and agrees that the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016

contains (1) digital files being true, exact, and accurate copies of the digital files found on the Original Digital Devices as they existed prior to them coming into the government's possession, and (2) true, exact, and accurate copies of digital file metadata contained on all Original Digital Devices as they existed prior to them coming into the government's possession – except for the Master File Table "file last access dates" corresponding to files accessed by the government via accessing the Original Digital Device named "filesalot.dcv" on August 3-4, 2008, prior to duplicating the device using reliable methods. *See* ¶ No. 2, *supra*. The government stipulates that no data within the destroyed data, *i.e.*, data *not* contained in the Necessary Digital Evidence Container File

having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016,

was previously physically shared with any other agent, agency, or entity within the government, with any other jurisdiction, or with any private party.

8. All Necessary Digital Evidence contained within the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016

is "admissible [into evidence] to the same extent as the original," within the meaning of Fed. R. Evid. 1003. The purpose of this stipulation is to establish an indisputable foundation for the Necessary Digital Evidence contained within the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016.

Therefore, defendant and the government may still dispute whether any particular piece of data is admissible in any proceeding.

9. All Necessary Digital Evidence contained within the Necessary Digital Evidence Container File having SHA-256 hash digest value:

ce57150435f62cfb0d72b08a869e31f2ccce153229cc15efc394aa4e25c7d016

may be admitted into evidence instead of the original material on the Original Digital Devices only in legal proceedings where the Original Digital Devices or their contents would be admissible. For example, if any of the Necessary Digital Evidence is ever suppressed based on a Constitutional violation, the government may not rely upon this stipulation to admit the suppressed Necessary Digital Evidence in a criminal trial where Daniel Rigmaiden is the defendant. Apart from the admissibility of the Necessary Digital Evidence, this stipulation itself and the facts agreed to herein may not be used to establish a fact in any proceeding that would otherwise require inadmissible evidence in order to be established. For example, if any of the Necessary Digital Evidence is ever suppressed based on a Constitutional violation, the government may not rely upon this stipulation itself, or the facts contained herein, as a substitute for the suppressed evidence in a

criminal trial where Daniel Rigmaiden is the defendant.

10. After the defendant has been sentenced in this case, his conviction has become final and the time for the defendant to file an appeal of the final judgment has expired, Internal Revenue Service – Criminal Investigations (IRS-CI) will then store all digital copies of the Necessary Digital Evidence. IRS-CI will then maintain the Necessary Digital Evidence in this manner for a period of 13 months. After that time period, the Necessary Digital Evidence will be destroyed by IRS-CI and defendant will be notified of the destruction via a signed IRS-CI report. If during that 13 month period the government wishes to share any information contained in the Necessary Digital Evidence with another agency or entity within the government, with any other jurisdiction, or with any private party, the government will notify the defendant and give him an opportunity to file an objection with the Court prior to any such sharing. The parties agree that, should the defendant file such an objection, the district court's resolution of the objection will be final and that neither party will have the right to appeal such resolution.

Respectfully submitted this 20th day of February, 2014.

JOHN S. LEONARDO
United States Attorney
District of Arizona

February 20, 2014
Date

FREDERICK A. BATTISTA
Assistant U.S. Attorney

January 27, 2014
Date

DANIEL D. RIGMAIDEN
Defendant